USDA PRIVACY IMPACT ASSESSMENT FORM

Project Name:
The Interactive Healthy Eating Index and Physical Activity Tool
Description of Your Program/Project: An online nutrition and physical activity assessment system that provides consumers feedback on their reported nutrition and/or physical activity status.

DATA IN THE SYSTEM

1. Generally describe the information to be used in the system in each of the following categories: Customer, Employee, and Other.	The system is used by the customers/employer.
2a. What are the sources of the information in the system?	1. Nutrient database for foods used in the Interactive Healthy Eating Index is based on the 1994-96, 98 Continuing Survey of Food Intakes by Individuals (CSFII) conducted by the Food Surveys Research Group of Agriculture Research Services at USDA. 2. Physical activity database for the activities used in the Physical Activity Tool is based on the Compendium of Physical Activities published by Ainsworth et al. (2000) in *Medicine and Science in Sports and Exercise*.
2b. What USDA files and databases are used? What is the source agency?	The nutrient database of the foods used in the system is based on the SR12 data with some food updates from SR14 both released by Agriculture Research Services of USDA.
2c. What Federal Agencies are providing data for use in the system?	The US Department of Agriculture.
2d. What State and Local Agencies are providing data for use in the system?	There are no data from State or Local Agencies used in the system.

2e. From what other third party sources will data be collected?	There are no data that will be collected from third party sources.
2f. What information will be collected from the customer/employee?	The foods eaten and physical activities performed by the consumers will be collected.
3a. How will data collected from sources other than the USDA records and the customer be verified for accuracy?	The data collected from sources other than USDA records are peer-reviewed by professionals and published online or in refereed journals. The data collected from the users are anonymous and only available to the individual. However, the data reported by the users cannot be verified for accuracy.
3b. How will data be checked for completeness?	Prior to the system's release to the public, the output data (i.e. tables, charts, and messages) are being beta-tested internally and pilot-tested by university students.

ACCESS TO THE DATA

1. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Other)?	User who can only access to his/her own data. Project Managers, System Administrator, and Developers have access right to the system data.
2. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?	The personal data can only be accessed by user-specific via a username and a password, which are created by the user him/herself. Detailed documentation on policies and responsibilities associated with accessing the system data on the database server are kept on file with the IT contractors at Digital Access Cooperation (DAC).
3. Will users have access to all data on the system or will the user's access be restricted? Explain.	The user can only access his/her own nutrition and physical activities analysis results on the system.
4. What controls are in place to prevent the misuse (e.g. browsing, unauthorized use) of data by those having access?	The consequences of using the data in unauthorized way by those having access to the system is also documented in details

	and kept on file with the IT contractors at Digital Access Cooperation (DAC). Additionally, all server accesses are logged.
5a. Do other systems share data or have access to data in this system? If yes, explain.	No
5b. Who will be responsible for protecting the privacy rights of the customers and employees affected by the interface.	The System Administrator at USDA FNS
6a. Will other agencies share data or have access to data in this system (International, Federal, State, Local, Other)?	No
6b. How will the data be used by the agency?	Only the aggregated web access data will be used by the owner agency for monitoring system usage purpose.
6c. Who is responsible for assuring proper use of the data?	The System Administrator at USDA FNS

ATTRIBUTES OF THE DATA

1. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?	Yes
2a. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?	No
2b. Will the new data be placed in the individual's record (customer or employee)?	N/A
2c. Can the system make determinations about customers or employees that would not be possible without the new data?	No

2d. How will the new data be verified for relevance and accuracy?	N/A
3a. If data is being consolidated, what controls are in place to protect the data from unauthorized access or use?	The System Administrator will provide aggregated data to the owner agency. No individual identifier can be accessed other than the System Administrator and the owner agency. Data are stored on a CD-ROM, which will be stored in a locked file cabinet and only the project managers have access to that information.
3b. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.	The data on the system are not being consolidated. Documentation on the proper controls is in place and kept with the IT personnel at DAC. There will be a System Administrator in place at all times.
4a. How will the data be retrieved? Can it be retrieved by personal identifier? If yes, explain.	Usernames, secure password hashes, and password hints will be stored on the system for users who wish to return to the site. After 3 failures of login attempts, the user will be promoted to enter his/her own password hint if the personal email address was provided to the system during the new user registration process. If the personal email was not given during the registration process, user is encouraged to re-register as a new user with a newly self-created username and a password. The password hint can be sent to the user via the personal email address if it is provided during the registration. Otherwise, forgotten usernames and/or passwords cannot be retrieved and new registration is encouraged.
4b. What are the potential effects on the due process rights of customers and employees of: • consolidation and linkage of files and systems; • derivation of data • accelerated information processing and decision making; • use of new technologies.	Customers can consolidate or link their personal assessment results only, based on what they have reported. Educational messages are linked to their nutrition and/or physical activity assessment. The users can decide how many times they wish to visit the site, follow the educational information or discontinue visit the site at any time. There is no known potential harm due to the use of new technologies.
4c. How are the effects to be mitigated?	There is no known adverse effect to be

	mitigated with use of the site.

MAINTENANCE OF ADMINISTRATIVE CONTROLS

1a. Explain how the system and its use will ensure equitable treatment of customers and employees.	Users who have access to the internet can visit the site at any time. There is no restriction on date and time usage of the site. However, there are minimum system requirements needed by users to browse the site properly. The user needs to have internet browser software installed on the computer, the screen setting needs to be at the minimum 256-color level, and screen resolution needs to be at least 800 x 600 pixels.
2a. If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?	Data are resided at the same location.
2b. Explain any possibility of disparate treatment of individuals or groups.	The site is compliance with the Section 508 requirement for disabilities equality access. English language is the only version of the site, which may be the possible disparate treatment for the users who visit the site.
2c. What are the retention periods of data in this system?	There is no restriction on the retention of user's data stored in the system for each of nutrition and physical activity assessment. Users can use the system as long as they wish. A list of frequently consumed foods or frequently preformed physical activity can be stored based on individual's preferences. A history of data entry points is stored on the system.
2d. What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented?	At the end of the retention period, automated SQL scripts are run on the database server to purge the system data it they are no longer needed. This process is done automatically and is documented via procedures on file with the IT personnel at DAC.
2e. While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?	When updated dietary and physical activity guidance is released, the nutrient and physical activity recommendations and educational messages will be updated accordingly.

3a. Is the system using technologies in ways that the USDA has not previously employed (e.g. Caller-ID)?	No
3b. How does the use of this technology affect customer/employee privacy?	User data assessment and analysis are based on what users report and enter into the system about their food intake and physical activity. Information provided by the users is considered personal and private.
4a. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.	The information related to the user is linked to a self-created username and password. Users can create or change to different unique usernames and passwords at any time, which can only be accessed by the user him/herself or the System Administrator.
4b. Will this system provide the capability to identify, locate, and monitor groups of people? If yes, explain.	The information provided by the system is only on an individual basis, not for groups of people.
4c. What controls will be used to prevent unauthorized monitoring?	Only the System Administrator has access to the system and is able to monitor the system usage when it is necessary.
5a. Under which Systems of Record notice (SOR) does the system operate? Provide number and name.	There is only a self-created username and password linked to the user's personal information, such as age, gender, weight and height for nutrition and physical activity assessment purposes. Date of data entry is also required for user who would like to track their nutrition and physical activity assessment results over times.
5b. If the system is being modified, will the SOR require amendment or revision? Explain.	N/A